

UNITED STATES DISTRICT COURT

FILED

for the
Eastern District of Missouri

JUN 20 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

Information associated with Facebook Inc. account:
[REDACTED] that is stored at premises owned,
maintained, controlled, or operated by Facebook Inc.

Case No. 4:19 MJ 287 DDN

APPLICATION FOR A SEARCH WARRANT

I, David J. Ogurek, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 USC 2251, 2252, 2252A

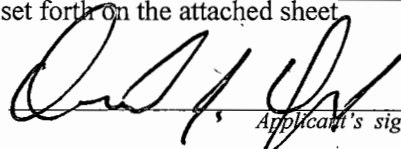
Offense Description

Production, possession and/or receipt, and shipment of child pornography, and other related materials

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Application's signature

David J. Ogurek, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: June 20, 2019

City and state: St. Louis, MO



Judge's signature

Honorable David D. Noce, U.S. Magistrate Judge

Printed name and title

AUSA: Robert F. Livergood

IN THE MATTER OF THE SEARCH OF:
Information associated with Facebook Inc.
account: www.facebook.com/100010497699733
that is stored at premises owned, maintained,
controlled, or operated by Facebook Inc.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David J. Ogurek, being duly sworn, do hereby depose and state:

I. INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (hereinafter referred to as "FBI"). I have been a Special Agent for approximately twelve years. My current assignment is with the Violent Crime/Organized Crime Squad where I am detailed to work on organized crime investigations. I have had numerous contacts and dealings with informants, victims and other individuals known to engage in organized criminal activity, to include drug trafficking, major theft, money laundering, and fraud. I have investigated and/or assisted in numerous investigations relative to federal cases concerning the above-listed offenses. As a Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. As a Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
4. The information contained within this affidavit is based on my training and experience, as well as information related to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not

included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Section 875(d), including but not limited to the items described on Attachments A and B, which are attached hereto and incorporated herein by reference, will be found within the Facebook Account held by **G.M.**, who uses the screen / user names for the account [REDACTED] where the instrumentalities, fruits and evidence of violations of Title 18, United States Code, Section 875(d), relating to the use of interstate or foreign commerce to communicate a threat to injure the reputation of a person with the intent to extort from them a thing of value, including but not limited to the items, as specified further in Attachments A and B, might be found.

5. This affidavit seeks a warrant to require **Facebook Inc.** located at 1601 Willow Road Menlo Park, CA 94025, to provide the contents of electronic mail and wire communications, including but not limited to, sent and received messages, photographs and videos, from and to **G.M.**, who uses the screen / user names for the account [REDACTED], for the time period of May 4, 2019 to the date of this warrant.
6. A warrant rather than a subpoena is necessary to obtain the desired information because **Facebook, Inc.** is arguably an “electronic communications service” and the contents of an electronic communication held in electronic storage by **Facebook, Inc.** for less than 180 days is arguably protected by the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et. seq.*
7. “Electronic communications service” means “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).
8. The term “electronic storage” means “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court (including a magistrate judge of such court) of the United States . . . that has jurisdiction over the offense being

investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY AND DEFINITIONS

10. Title 18, United States Code, Section 876(d) criminalizes the use of interstate or foreign commerce to communicate a threat to injure the reputation of a person with the intent to extort from them a thing of value.

II. STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

11. Title 18, United States Code, Sections 2701 through 2711, is entitled “Stored Wire and Electronic Communications and Transactional Records Access.”

- a. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

- b. Title 18, United States Code, Section 2703(b) provides, in part:

- (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
 - (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the procedures described in the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant...

- (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service –
- (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
- (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
- c. The government may also obtain records and other information pertaining to a subscriber or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).
- d. The presence of an officer is not required for service or execution of a search warrant issued in accordance with Chapter 121, Title 18 of the United States Code requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service. 18 U.S.C. § 2703(g).
- e. Title 18, United States Code, Section 2711, provides, in part:
- As used in this chapter –
- (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and
- (2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

f. Title 18, United States Code, Section 2510, provides, in part:

- (1) “contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;
- (2) “electronic communications system” means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications;
- (3) “electronic communication service” means any service, which provides to users thereof the ability to send or receive wire or electronic communications;
- (4) “electronic storage” means –
 - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 - (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

III. BACKGROUND

12. The following terms have the indicated meaning in this affidavit:

- a. The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).
- b. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of

the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person. 18 USC § 2256(2).

- c. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).
- d. The Internet is in part a computer communications network using interstate and foreign telephone lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive graphic image files.

III. FACEBOOK BACKGROUND

- 12. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
- 13. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.
- 14. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
- 15. Facebook users can select different levels of privacy for the communications and

information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

16. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.
17. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.
18. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

19. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.
20. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.
21. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.
22. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.
23. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.
24. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.
25. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
26. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users.

Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

27. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).
28. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

IV. INVESTIGATION

30. On May 9, 2019, this affiant and Investigator Donya Jackson with the United States Attorney's office became aware of incident involving victim G.M. On May 10, 2019, Investigator Jackson interviewed G.M and her sister, M.M., and obtained the following information.
31. On the evening of May 8, 2019, G.M. received a Facebook communication from a subject named "Allison Lewis." G.M believed she knew "Allison Lewis" and began communicating with "Allison Lewis" through the Facebook Messaging application on her cell phone.
32. The conversation turned sexual and "Allison Lewis" requested that G.M. take her clothes off and participate in a Facebook video chat. This feature allows each user to see the other user while talking. G.M. proceeded to get nude and engaged in the video chat feature with "Allison Lewis." G.M. stated that she was talking and engaging with a real person she believed to be a female during the video chat.
33. After the video chat ended, G.M. started to receive harassing messages from "Allison Lewis" calling her "Retarded" and threatening to ruin her life. "Allison Lewis" then messaged naked screenshots of G.M. in sexual poses that were taken during the video chat.
34. G.M. stated that she became upset and showed these messages to her older sister, M. M. M.M. began contacting "Allison Lewis" via her own cell phone and Facebook account. M.M. received these messages:

Allison Lewis: "If you really want me to delete your video, I want you to pay some money to my mother who is sick for her medical care ??

M.M: "This isn't Allison. This is fake. Delete those videos. Now.

Allison Lewis: "so you really want to see what I'm really capable of doing with your sister's video now"

Allison Lewis: "You have just 10 seconds to answer me or I swear to start has published the video on the net" "1s" "2s" "3s" "4s" "5s" "6s" "7s"

35. Both G.M. and M.M. blocked the Facebook account of "Allison Lewis."
36. Preservation requests were submitted and received by Facebook for both accounts belonging to G.M. and M.M.
37. G.M. consented law enforcement to access her Facebook account but in order to obtain complete Facebook records a search warrant is requested.
38. Based on the above information, there is probable cause to believe that the items listed in Attachment A constitute evidence of violations of Title 18, United States Code, Section 875(d) and will be found in the electronic or wire communications stored by **Facebook Inc.** located at 1601 Willow Road Menlo Park, CA 94025.
39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



DAVID J. OGLUREK
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 20th day of June, 2019.



DAVID D. NOCE
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

For the period of May 1, 2019, to June 19, 2019, this warrant applies to information associated with the Facebook account [REDACTED] that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the accounts and all other documents showing the users' posts and other Facebook activities from May 1, 2019, to June 19, 2019;
- (c) All photos and videos uploaded by the users IDs and all photos and videos uploaded by any user that have that user tagged in them from May 1, 2019 to June 19, 2019, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records of communications and messages made or received by the users, from May 1, 2019, to June 19, 2019, including all Messenger activity, private

messages, chat history, video and voice calling history, and pending "Friend" requests;

- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the accounts;
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the accounts are or were a "fan" of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account from May 1, 2019, to June 17, 2019;
- (m) All information about the users' access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within **14 DAYS** of service of this warrant. The information should be sent by **Federal Express or the law enforcement portal to Special Agent David J. Ogurek at the FBI located at 2222 Market Street, St. Louis, MO 63103.**

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U. S.C. § 875(d) from May 1, 2019, to June 19, 2019, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) The identity and location of the person(s) using the name “Allison Lewis;”
- (b) All communications received from or sent to “Allison Lewis;”
- (c) All pictures or videos received from or sent to “Allison Lewis;”
- (d) All communications that are threatening or harassing;
- (e) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (f) Evidence indicating “Allison Lewis” state of mind as it relates to the crime under investigation;
- (g) The identity of the person(s) who created or used the name “Allison Lewis,” including records that help reveal the whereabouts of such person(s);
- (h) Correspondence between any Facebook account where the content of the message discusses threats or harassment;
- (i) Correspondence between any Facebook account where the content of the message includes naked or partially naked persons;
- (j) Any message, opened or unopened, and any image file involving the threats or harassment of any person;
- (k) Any message, opened or unopened, and any image file that appears to contain passwords or information regarding encryption;
- (l) Any and all transactional information, to include log files (transmission and usage), of all activity of the accounts which includes dates, time, method of connecting, port, dial-up, and/or location, originating Internet Protocol (IP) address and the destination IP address for all opened and unopened email, during

the entire period that the account has been active, including buddy lists and terms of service violation reports; and

- (m) Any records of subscriber information, method of payment, or detailed billing.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature